CHAPTER

8

INTERNETWORKING WITH REMOTE ACCESS

After reading this chapter and completing the exercises, you will be able to:

- Understand remote access under Windows XP
- Configure various remote access connection types for a Windows XP Professional system
- Install remote access hardware
- Understand remote access security
- Understand the Internet Options applet
- Implement Internet Connection Sharing and the Internet Connection Firewall
- Understand the native Internet tools and utilities
- Troubleshoot remote access problems

Not all network access occurs from computers that are directly attached to the network where the resources and data reside. For roaming workers, such as salespeople and field engineers, and increasingly for telecommuters, the ability to gain access to a network remotely—that is, from some location other than where the network physically resides—is crucial. This is an area where Windows XP really shines; it is one of the few major network operating systems that includes remote access capabilities with the core software at no additional charge. For Windows XP Professional, this means that part of the package is a single dial-in or dial-out connection that can use a **modem** over a PSTN (Public Switched Telephone Network) connection, DSL (Digital Subscriber Loop), cable modem, an **ISDN (Integrated Services Digital Network)** line, frame relay, or any of the other more exotic digital remote link technology. Since Windows NT became a force to be reckoned with in 1995 with the release of Windows NT 3.51, remote access services have played a central role in the operating system's burgeoning popularity and widespread acceptance up to and including the current Windows XP release.

REMOTE ACCESS

You can use **remote access service** to logon to a Windows XP system for user or administrative access while you're away from the office. For example, a user can access the system from a hotel room while traveling on business. Remote access can be used to dial into another system or to answer incoming connections. A client system is any system that initiates access to a Windows XP system established as a remote access server.

A Windows XP remote access configuration includes the following components:

- *Clients*—Windows XP, Windows 2000, Windows NT, Windows 95/98, Windows for Workgroups, MS-DOS (with Microsoft network client software installed), and LAN Manager remote access clients can all connect to a Windows XP remote access server. "Clients" can also mean any client of a platform that supports the Point to Point Protocol (PPP).
- *Protocols*—Windows XP remote access servers support the PPP protocol, enabling any PPP client to use TCP/IP (Transmission Control Protocol/Internet Protocol) or NWLink (IPX/SPX). Windows XP as a dial-up client can also access the installed base of SLIP (Serial Line Internet Protocol) remote access servers. However, SLIP cannot be used to connect to a Windows XP remote access server system.
- *WAN Connectivity*—Clients can dial in using standard telephone lines with a modem or modem pool employing legacy analog or the new DSL technology. Faster links are possible using ISDN or T-Carrier lines. Remote access clients can also be connected to remote access servers using X.25, ATM (Asychronous Transfer Mode), or an RS-232C null modem. Windows XP also allows for Channel Aggregation with PPP Multilink. Windows XP does support cable modems; however, in most cases proprietary software and drivers from the vendor are used to establish connections over these network adapter-like devices, because they function differently from a modem.
- *Security*—Windows XP logon and domain security, support for security hosts, data encryption, Internet Connection Firewall (ICF), IPSec (IP Security), and callback provide secure network access for remote clients. With Windows XP you also have the option of separating LAN traffic from remote access traffic with the Point-to-Point Tunneling Protocol (PPTP) or the Layer Two Tunneling Protocol (L2TP).
- *Server*—As a remote access server, Windows XP Professional supports only one inbound connection at a time. However, most Windows Server operating systems permit up to 256 remote clients to dial in. The remote access server can be configured to provide access to an entire network or restrict access to the remote access server.
- *LAN protocols*—IP protocol support permits accessing a TCP/IP network like the global Internet. NWLink (IPX/SPX) protocol support enables remote clients to access NetWare servers and printers. You can use NetBIOS

applications over IPX or TCP/IP, and Windows Sockets applications over TCP/IP or IPX, named pipes, Remote Procedure Call (RPC), and the LAN Manager API are also supported.

Remote control and remote access are control technologies that work in different ways. Remote control employs a remote client as a dumb terminal for the answering system, whereas remote access establishes an actual network connection between a remote client and the answering computer system, using a link device (such as a modem) as a network adapter. Remote access keyboard entries and mouse movements occur locally; with remote control, these actions are passed to a host system. Using remote access, computing operations are executed on the client; remote control computing operations are executed on the host with the resulting video signal sent to the client.

Remote access and Terminal Services are also different mechanisms. Terminal Services allows thin clients—basic computers consisting of a display, keyboard, and mouse, with only enough capability to connect to the terminal server host—to participate in a rich computing environment. Basically, the terminal server host acts as the CPU for the thin client. All operations and calculations are performed on the terminal server host; only display changes are sent to the client and only keyboard and mouse information is sent back to the terminal server. Terminal Services are often employed in situations where budget restrictions prevent the purchase of fully capable desktop systems or when complete security is required (i.e., when data cannot exist outside the secure server). Remote access is a mechanism by which remote computers that exist as independent systems are able to make connections over some type of communication link to a system or standalone machine. This link is used to access data or to gain further access to linked networks.

Features of Remote Access in Windows XP

Remote access is a standard component of Windows XP and does not require a manual service installation. Some of the impressive features of remote access under Windows XP are discussed in the following sections.

PPP Multilink

PPP remote access multilink allows you to increase overall throughput by combining the bandwidth of two or more physical communication links such as analog modems, ISDN, and other analog/digital links. PPP Multilink is based on Internet Engineering Task Force (IETF) standard RFC 1717, "The PPP Multilink." RFC stands for Request for Comments, designating official standards documents published by the IETF. This standard is located on the Web at *http://www.faqs.org/rfcs/rfc1717.html*.

VPN Protocols

Windows XP supports two virtual private network (VPN) protocols: Point-to-Point Tunneling Protocol and Layer Two Tunneling Protocol. **Point-to-Point Tunneling Protocol (PPTP)** is a networking technology that supports multiprotocol VPNs, allowing users to access corporate networks securely through the Internet. Clients using PPTP can access a corporate LAN by dialing an ISP or directly through the Internet. In both cases, the PPTP tunnel is encrypted and secure and works with any protocol.

Cisco Systems developed a PPTP alternative called **Layer Two Tunneling Protocol (L2TP)**. Similar to PPTP, L2TP encapsulates PPP frames for transport over various networks, including IP, X.25, Frame Relay, and ATM. L2TP is used in combination with IPSec to provide a secure encrypted VPN link over public networks.

Restartable File Copy

The restartable file copy feature automatically retransmits incomplete file transfers produced by interruption of remote access connectivity. This feature provides the following:

- Faster transmission of large files over lower-quality connections
- Reduced cost from avoiding retransmission of the whole file
- Reduced frustration from interrupted transfers

Idle Disconnect

The idle disconnect feature breaks off a remote access connection after a specified period of inactivity. This feature reduces the costs of remote access, helps you troubleshoot by closing dead connections, and frees up inactive remote access ports.

Autodial and Log-on Dial

You can configure remote access to automatically connect and retrieve files and applications stored on a remote system. Users do not have to establish a remote access connection each time they want to transfer a remote object; Windows XP quickly and efficiently handles all remote access events. By maintaining a virtual database of mappings between resources and connection objects, Windows XP remote access is able to re-establish links when previously accessed resources are re-requested.

Client and Server Enhancements

Windows XP remote access includes a number of client and server components that allow third-party vendors to develop remote access and dial-up networking applications.

Look and Feel

Windows XP remote access has undergone some changes since Windows 2000 and is significantly different from similar utilities in Windows NT and Windows 95/98. Remote access capabilities have now been integrated with the networking components, resulting in Network Connections, a multi-purpose management interface where both standard LAN networking links and remote access links are established and configured. Just about everything related to remote access is controlled through this interface. The only exception is that all remote access hardware (such as modems) are installed through the Add Hardware applet if they were not installed automatically by plug and play at bootup.

Callback Security

You can control access to the system from specified phone numbers by using the Callback feature. Calls may originate only from known phone number locations, or the remote access client can set the phone number dynamically. Callback is configured on the Callback tab of the Dial-up Preferences dialog box accessed through the Advanced menu of the Network Connections utility. There are three options: No callback, Ask me during dialing when the server offers, and Always call me back at the number(s) below. Allowing the number to be set dynamically (i.e., during the connection) does not provide any security; security is enforced only when predefined callback numbers are used.

WAN Connectivity

Wide area networks (WANs) link sites that are often a considerable physical distance apart. Using remote access, Windows XP enables you to create a WAN by connecting existing LANs through remote access over telephone, ISDN, cable modems, campus networks, or other communication lines. This is a cost-effective solution if you have minimal-to-moderate network traffic between sites. You can improve the performance of remote access-based WANs in one of three ways:

- Increasing bandwidth of the remote access connection
- Multilinking communication links using PPP Multilink
- Implementing PPTP over the Internet

Internet Network Access Protocols

Windows XP remote access supports all standard protocols for remote Internet access as well as **PPP Multilink**, a variation of PPP that enables you to create one large high-bandwidth pipe by banding together multiple PPP channels. The remote access protocol used in establishing and maintaining a WAN link is dependent on the client and server OS and LAN protocols. Windows XP-supported remote access protocols are outlined in the following sections.

PPP

Point-to-Point Protocol (PPP) is the current standard for remote access. Remote access protocol standards are defined in RFCs published by the IETF and other working groups. The RFCs supported in Windows XP remote access are:

- *RFC 1661*—The Point-to-Point Protocol (PPP)
- *RFC 1549*—PPP in HDLC Framing
- *RFC 1552*—The PPP Internetwork Packet Exchange Control Protocol (IPXCP)
- *RFC 1334*—PPP Authentication Protocols
- *RFC 1332*—The PPP Internet Protocol Control Protocol (IPCP)

Microsoft recommends using PPP because it is flexible and is the industry standard, which means continued compatibility with client and server hardware and software in the future. Remote clients connecting to third-party PPP servers might need to use a post-connect terminal script to logon to the PPP server. The server informs users it is switching to PPP framing mode (users must start the Terminal to complete logon).

When using a non-Microsoft PPP stack to dial into a Windows Server that is a part of a domain and not a domain controller, the server looks only to its local accounts for the account name and password you specified on dial-in. If the server doesn't find the name and password locally, it won't check the domain accounts; it simply denies access. Because a domain controller does not have local accounts that it can use for verification, it uses the accounts in the domain's Active Directory database to grant or deny access.

PPTP

Point-to-Point-Tunneling Protocol (PPTP) is one of Windows XP's most interesting features. It allows you to establish a secure remote access pipeline over the public Internet and to "tunnel" IPX or TCP/IP traffic inside PPP packets. PPTP can provide real benefits for companies with numerous remote users who now subscribe to a local Internet Service Provider (ISP) for e-mail and Internet access and who use the same connection to access the corporate LAN. These VPNs can support the IPX and TCP/IP LAN protocols and provide private network access from any Internet connection point. PPTP's significant features include:

- *Transmission costs*—Uses the Internet as the primary long-distance connection medium rather than leased lines or long-distance telephone lines, reducing the cost of establishing and maintaining a remote access connection.
- *Hardware costs*—Requires less hardware by letting you locate modems and ISDN hardware on a network rather than directly attaching them to the remote access server.

- *Administrative overhead*—Permits centralized management of remote access networks and users.
- *Improved security*—Connections over the Internet are encrypted and secure.

L2TP is a similar protocol developed by Cisco for use with IPSec to support secure VPN links. From a user's perspective, it operates in the same manner as PPTP.

PPP-MP

The **PPP multilink protocol (PPP-MP)** combines two or more physical remote access links (modem, ISDN, or X.25 links) into one logical bundle with greater bandwidth. Multilink can combine analog and digital links in the same logical bundle. The only drawback to multilink is that all connections to be aggregated must be of the same technology type. For example, ISDN and modem links cannot be aggregated, but three ISDN lines can.

Because only one phone number can be stored in a user account, Multilink does not function with the callback security feature.

SLIP

Serial Line Internet Protocol (SLIP) was one of the first protocols developed specifically for TCP/IP support over dial-up connections. Though SLIP is rarely used (PPP offers much more power and flexibility), Microsoft has included it in Windows XP for backward-compatibility with older systems. SLIP does not support the Dynamic Host Configuration Protocol (DHCP), so a static IP address must be assigned to every SLIP client, making IP address administration more difficult. Unlike PPP, SLIP does not support IPX. SLIP's biggest drawback is that it does not support encrypted passwords; SLIP passwords are passed as plain text. Windows XP remote access does not offer a SLIP server, but supports SLIP as a client.

The RFCs supported by remote access SLIP are:

- *RFC 1144*—Compressing TCP/IP Headers for Low-Speed Serial Links
- *RFC 1055*—A Nonstandard for Transmission of IP Datagrams Over Serial Lines: SLIP

Telephony Features

TAPI, the remote access Telephony API, supplies a uniform way of accessing fax, data, and voice. TAPI is part of the Windows Open System Architecture (WOSA) developed

to aid third-party vendors in designing powerful, integrated telephony applications. TAPI enables communication between a TAPI-aware computer and telephone hardware, such as PBX, modems, and fax machines. TAPI treats a telephone network as a system resource using standard APIs and device drivers, so once installed, TAPI applications have seamless access to phone features and server-based communications.

Remote Access Configuration

As stated previously, remote access is an integrated default component of Windows XP, and no additional service installation is required. Remote access is configured and managed from the Network Connections window (see Figure 8-1). The basic functions of this window were discussed in Chapter 7, "Network Protocols" (refer to that discussion for general interface information). This interface window is accessed through the Start menu by selecting Start | Control Panel, clicking Network and Internet Connections (if in Category view), then clicking Network Connections.

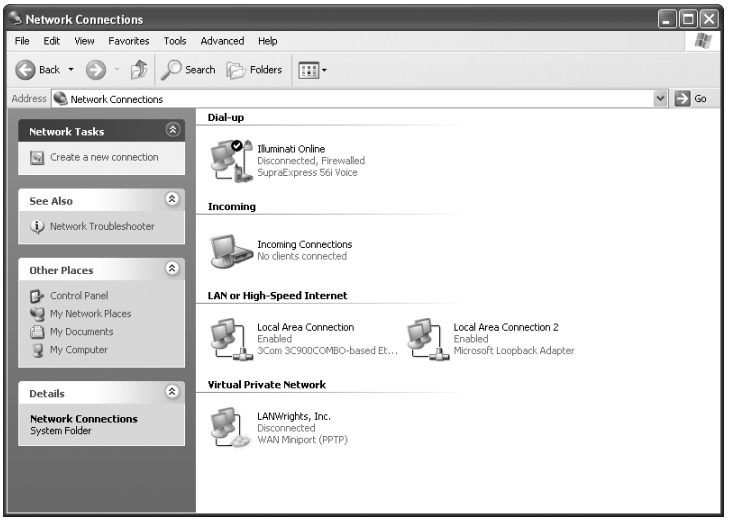

Figure 8-1 Network Connections

All remote access or remote links must be created. The New Connection Wizard is launched by clicking the Create new connection link in the Network Tasks list. The second page of this Wizard offers three remote connection options (see Figure 8-2):

Figure 8-2 New Connection Wizard

- *Connect to the Internet*—Creates a connection object to connect to an ISP.
- *Connect to the network at my workplace*—Creates a connection object to connect to a network through dial-up or VPN.
- *Set up an advanced connection*—Creates a connection object using a serial, parallel, or infrared port connection, or configures the system to answer incoming connections.

Establishing remote access connection objects using the Wizard is very elegant and quick. In the following sections, we look at the step-by-step process for each of these connection types and the post-creation properties you can manipulate.

All the following network connection types require that the hardware device used to establish the remote access link be pre-installed and configured before creating the connection object. This includes modems, cable modems, ADSL devices, infrared ports, etc. See the section titled "Installing Remote Access Hardware" later in this chapter for information on device installation.

Connecting to the Internet

The Internet has quickly become the communication medium of the masses. It's difficult to watch a television show or listen to the radio without hearing about a Web site or an e-mail address. Microsoft had the foresight to include Internet access as a standard component of Windows XP remote communications. Windows XP also includes Internet Explorer and Outlook Express, in addition to the other common TCP/IP utilities often used over the Internet (i.e., FTP, Telnet, ping, tracert, etc.).

The Connect to the Internet Wizard selection can be used to:

- *Choose from a list of Internet service providers (ISPs)*—Establish a new account through MSN or an ISP that services your area.
- *Set up my connection manually*—Set up an ISP connection manually whether connecting using a dial-up phone number (such as analog modem, ISDN, or DSL) or a broadband always-on connection (such as cable modem).
- *Use the CD I got from an ISP*—Launch an ISP installation from a vendor-provided CD.

Transferring an existing MSN account to this computer involves the use of the File and Transfer Wizard as discussed in Chapter 5, "Users, Groups, Profiles, and Policies."

To create a connection object for Internet access, follow the steps described in Hands-on Project 8-2.

Once a connection object is created, the Connect dialog box is automatically launched and offers four action buttons at the bottom of its display. The Dial button launches this connection and attempts to establish a connection using the current settings. The Cancel button closes the Connect dialog box and discards any changes made. The Properties button opens the multi-tabbed Properties dialog box for this connection object. The Help button launches the Windows XP Help system in the Network Connections context section.

In most cases you'll want to click Dial to test the new object. If your modem was properly configured, your phone line attached, and the service was not offering a busy signal, you should have established an Internet connection, and the default homepage should be displayed in Internet Explorer. Close Internet Explorer by selecting Close from the File menu. You might be prompted to terminate your connection; choose No to keep the connection active for now. Notice the connection icon in your icon tray—it's the one with the two overlapping monitors that blink. Double-clicking this icon opens the connection status dialog box (see Figure 8-3). You can terminate the connection at any time by clicking the Disconnect button in this dialog box. This same connection status dialog box can be accessed by double-clicking on a connection object from the Network Connections utility.

The connection status dialog box's General tab displays connection status, duration, speed, packets (LAN connections), bytes (dial-up connections), compression (dial-up connections), and errors (dial-up connections). From this tab you can access the connection object's Properties or Disconnect the link. The Details tab lists data relevant to the connection, such as server type, protocols, and IP addresses of server and client.

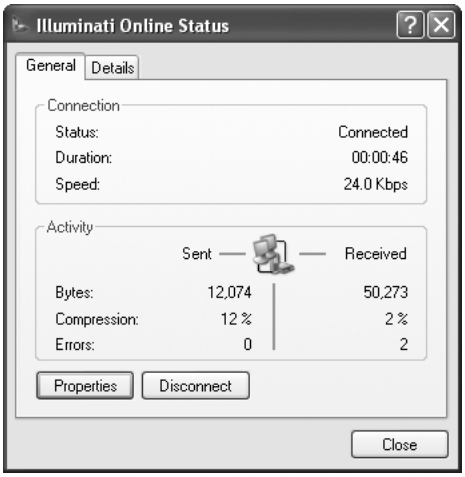

Figure 8-3 The Connection Status dialog box

If your system employs a proxy server to gain Internet access over a LAN, you will not see a connection object representing the proxy connection in the Network Connections window, nor will a connection status icon appear in the icon tray. Proxy connections are defined through the LAN Settings button on the Connection tab of the Internet Options applet (the Internet Options applet is accessed through the Control Panel or the Tools menu in Internet Explorer). Any changes to your proxy settings should be made through the LAN Settings dialog box.

The connection object functions on default settings in most cases, but you might want to fine-tune your connection to improve performance or add capabilities. The Properties dialog box for a connection object can be accessed through a variety of means:

- Select the connection object in the Network Connections window, then select Properties from the File menu or right-click the icon and select Properties from the pop-up menu.
- If the connection object is already in use, right-click the tray icon and select Properties from the pop-up menu.
- If the connection object is already in use, double-click the tray icon, then click the Properties button on the Status dialog box.

No matter how you get there, the Properties dialog box (see Figure 8-4) for an Internet connection object is used to configure a wide variety of settings that were not offered by the creation Wizard.

Figure 8-4 A connection object's Properties dialog box, General tab

The General tab is used to configure devices and dial-up numbers. The Connect using field lists all installed communication devices. Those devices with a marked checkbox are employed by the connection object in an attempt to establish a connection. The listed devices can be ordered to give priority to the faster or more reliable devices. By default, all devices dial the same phone number. By deselecting the All devices call the same number checkbox; the Phone number area becomes dependent on the selection of a device. The Phone number area includes settings for the area code, phone number, country/region code, and dialing rules (see the "Phone and Modem Options" section later in this chapter). Individual devices can be configured by clicking the Configure button when a device is selected. This opens a device-specific configuration dialog box where elements such as communication speed, modem protocols, hardware features, terminal window, logon scripts, and modem speaker are configured.

Settings on this dialog box apply only to the selected device. The Show icon in notification area when connected checkbox enables an icon for this connection to appear in the icon tray. This icon is used for quick access to connected links.

The Options tab (see Figure 8-5) configures the behavior of the connection object while establishing a connection. The settings are:

Figure 8-5 A connection object's Properties dialog box, Options tab

- *Display progress while connecting*—Provides a status report of the connection establishment process; default is selected.
- *Prompt for name and password, certificate, etc.*—Forces access credentials before launching the connection object; default is selected.
- *Include Windows logon domain*—Forces the connection to request logon domain information from the remote access server; default is not selected.
- *Prompt for phone number*—Forces the connection object always to prompt for phone number verification before attempting to establish a connection; default is selected.
- *Redial attempts*—Sets the number of retries the system will make when a connection cannot be established with the remote system; default is three retries.
- *Time between redial attempts*—Sets the time period between redials; default is one minute.
- *Idle time before hanging up*—Sets the inactivity disconnect time period; default is never.
- *Redial if line is dropped*—Forces the connection object to attempt to reconnect if the link is broken for any reason; default is enabled.

- *Multiple devices*—Enables multilink; default is Dial all devices. Other settings include Dial only first available device (establishes a single link with the remote system) and Dial devices only as needed (establishes activity-based dialing). Clicking the Configure button for the latter selection opens the Automatic Dialing and Hanging Up dialog box (Figure 8-6), which is used to define when additional devices are dialed or disconnected based on level and time period of traffic. Defaults are dial new devices when current bandwidth has been at 75% utilization for two minutes, and to disconnect when utilization has been less than 10% for two minutes.

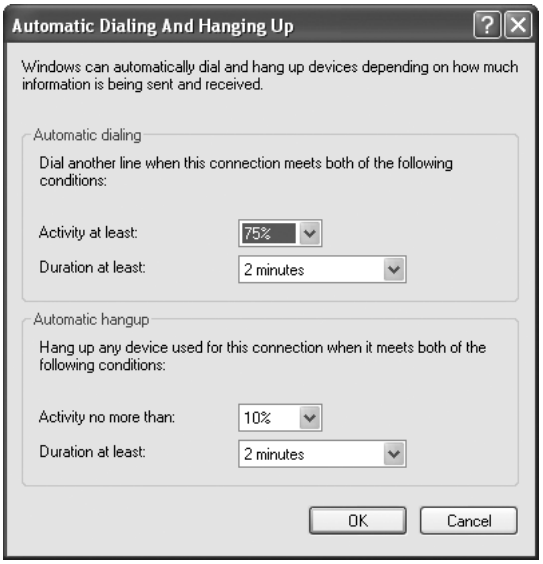

Figure 8-6 The Automatic Dialing And Hanging Up dialog box

- ***X.25***—Opens the configuration dialog box for X.25 connections, through which you can define the X.25 network type in use, your X.25 address, and the two optional settings of user data and facilities. For more information on X.25, consult the *Microsoft Windows .NET Server Resource Kit*.

The Security tab (see Figure 8-7) is used to define the connection object's security requirements. This tab offers two top-level security settings: Typical (recommended settings) and Advanced (custom settings). The default setting is the Typical, which allows unsecured passwords. This top-level setting has two other options: Require secured passwords and Use smart cards. Two checkboxes further define these alternate security options. The Automatically use my Windows logon name and password (and domain if any) checkbox should be used when your local and remote logon credentials are identical (this checkbox is enabled only when Require secured password is used). The

Require data encryption (disconnect if none) option protects not just the authentication process but all data transferred over the link (this checkbox is not enabled when Allow unsecured password is used).

Figure 8-7 A connection object's Properties dialog box, Security tab

The second top-level security setting, Advanced (custom settings), is used to specify exactly the level of security for this connection object. The Settings button reveals the Advanced Security Settings dialog box (see Figure 8-8), which offers the following settings:

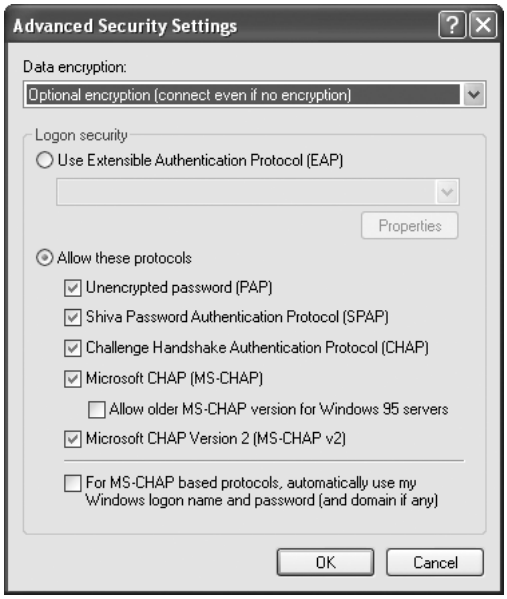

Figure 8-8 The Advanced Security Settings dialog box

- *Data encryption*—Defines the encryption requirements. Selections are No encryption allowed (server disconnects if it requires encryption), Optional encryption (connect even if no encryption), Require encryption (disconnect if sever declines), and Maximum-strength encryption (disconnect if server declines).
- *Use Extensible Authentication Protocol (EAP)*—Enables smart card or third-party security mechanisms to be required. The Properties button accesses mechanism-specific configuration settings. Windows XP includes default drivers for smart card readers and MD5-challenge mechanisms. See the *Microsoft Windows .NET Server Resource Kit* for more details on smart cards and third-party security mechanisms.
- *Allow these protocols*—Selects the encryption protocols allowed over this connection object, including PAP (i.e., unencrypted clear text), SPAP, CHAP, MS-CHAP, MS-CHAP from Windows 95, and MS-CHAP v.2.
- *For MS-CHAP based protocols, automatically use my Windows logon name and password (and domain if any)*—Uses local logon credentials over the connection object.

Defining custom security settings can be an intricate process. We recommend consulting the *Microsoft Windows XP Professional Resource Kit* for more information on custom security settings before attempting to deploy a custom security scheme on your network or over your remote access connections.

The bottom of the Security tab controls whether to pop up a terminal window and run a script after a connection is established. These settings apply to all devices used by this connection object. To define device-specific items, use the Configure button on the General tab. In most cases, terminal windows and logon scripts are unnecessary; however, depending on the type of server you are connecting to and the security mechanisms employed, you might need to alter these settings. A terminal window allows you to enter keystrokes directly to the authentication mechanism on the remote server. Some systems require multiple passwords, selecting a logon method from a menu, or issuing protocol launch commands. If the logon requirements of a system can be automated, you can create a logon script that provides these items automatically without requiring a terminal window and user input each time the connection is established. Dial-up logon scripts can be as complex as necessary, including branching decision trees based on data from the remote server. Windows XP includes several sample scripts in the %systemroot%\System32\ras\ folder that you can customize for your own purposes. For details on creating and modifying logon scripts, consult the content of the sample scripts (which include useful details in the form of context specific comments) and the *Microsoft Windows XP Professional Resource Kit*.

The Networking tab (see Figure 8-9) is used to configure the network communication components employed by the connection object. As you can see, this tab is very similar to the Properties of a Local Area Connection object. Because a remote access connection is the same as a local connection and differs only in speed, this similarity is not surprising.

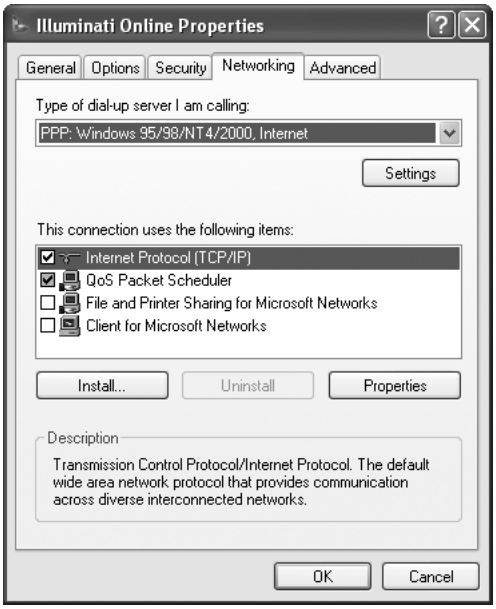

Figure 8-9 A connection object's Properties dialog box, Networking tab

The most important setting on this tab is the type of dial-up server. Your options are PPP and SLIP. Because Windows remote access servers can accept only inbound PPP connections, you'll most likely select PPP. However, if you are connecting to an older UNIX system, you might need to employ SLIP. If you don't know, try PPP first, because it is the standard remote link connection technology. PPP offers three further configuration details through the Settings button: enabling LCP extensions, enabling software compression, and negotiating multilink for single-link connections. In most cases the default settings are correct, but when connecting to older UNIX or other platforms, these PPP settings can prevent stable communications.

The remaining portion of this tab is used to enable, install, and configure networking components. Enabling and disabling a component applies only to this connection object, but installing or removing a component applies to all connection objects. By default, only the Internet Protocol (TCP/IP) and QoS Packet Scheduler components are enabled; the File and Print Sharing for Microsoft Networks component is disabled. For information on configuring networking components, refer to Chapter 7.

The Advanced tab (see Figure 8-10) is used to configure Internet Connection Firewall (ICF) and Internet Connection Sharing (ICS) for this connection object. ICF offers a reliable level of security for Internet connections. ICS is used to share a single Internet connection with other computers on your network. ICF and ICS are discussed later in this chapter.

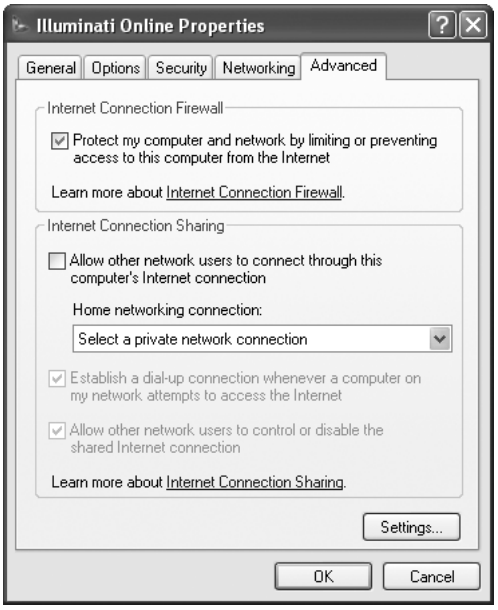

Figure 8-10 A connection object's Properties dialog box, Advanced tab

Connecting To The Network At My Workplace

Telecommuters and mobile personnel often need to communicate with the office LAN for a wide variety of purposes. Because a remote access link supports all network functions (access to files, printers, proxied Internet access, security control, service access, network application interaction, etc.) with only a change in the speed (based on the connection technology), remote connections to the LAN are very useful. Many organizations are taking advantage of the ease of distance communications offered by Windows XP, Windows 2000, Windows NT, and Windows 9x to reduce office space costs and increase the productivity of their employees.

Virtual private networking (VPN) is a trend in mobile computing that employs the Internet as a long-distance carrier to enable distant secure LAN connections. VPNs enable mobile or remote computers to establish a connection with a LAN over a local connection to an ISP. In other words, you can connect to the Internet anywhere in the world through a local access point, then use Windows XP VPN technology to link to your LAN. Such a remote access link offers you all of the functionality of a network client, with only slightly reduced speed. Furthermore, Windows XP VPN encrypts not just your authentication credentials, but all of the data transferred as well, thus ensuring private, secure, confidential long-distance computing.

The Connect to the network at my workplace option on the second page of the New Connection Wizard (see Figure 8-2) is used to create direct dial-up and VPN connections to an office LAN. Keep in mind that a VPN link establishes a PPTP or L2TP communication pipeline over an existing network connection between two systems. Thus, you must either have a dedicated LAN or use a dial-up connection to establish the network between the two systems to be linked.

To create a connection object on a client to be used to connect to a remote access server, follow the steps in Hands-on Project 8-1. To create a VPN connection object, follow the steps in Hands-on Project 8-3.

The Properties dialog box of a network dial-up connection object is substantially the same as that of a Internet ISP connection object. The only real difference is that the network dial-up connection object has the Client for Microsoft Networks component enabled on the Networking tab, and the ISP connection object does not. Refer to the previous connection object section for details on the Properties dialog box for network dial-up connection object.

The Properties dialog box of a VPN connection object is similar to that of a Internet ISP connection object, with a few distinct differences. The General tab lists the IP address or host name of the VPN server and controls whether an Internet connection is dialed before attempting the VPN connection. The Options tab does not include X.25 options. The Security tab does not include terminal window and script options, but does include a button to enter the IPSec Security pre-shared authentication key. The Networking tab defines the type of VPN to establish; the options are Automatic, PPTP VPN, and L2TP IPSec VPN.

The remote access server to which you are connecting must be pre-configured to accept VPN connections. See the "Setting Up An Advanced Connection" section to learn how to configure a Windows XP system to accept inbound connections.

Setting Up An Advanced Connection

The Set Up An Advanced Connection option on the second page of the New Connection Wizard can be used to establish a direct connection between two systems or configure the system to answer inbound dial-up calls. Because these are very different activities, they are discussed in separate sections to follow.

Accepting Incoming Connections

Windows XP Professional, although designed as a network client, can act as a remote access server for a single incoming connection. That connection can be made over a modem, existing Internet/network connection (i.e., a VPN link), or a direct access cable. In most cases, you'll use this feature only for special-purpose applications. For example, accepting a dial-in connection can be used to access your home system while traveling or to simplify technical support help for telecommuters. To configure Windows XP to accept incoming connections, follow the steps in Hands-on Project 8-4.

The process of configuring an incoming connection object includes the selection of the devices that answer incoming calls, whether to allow VPN links, which users can dial in, and which networking components (protocols, clients, and services) are supported over a dial-in link. Once that's completed, the incoming connection object is added to the Network Connections window. Opening this object's Properties reveals a three-tabbed dialog box. The General tab (see Figure 8-11) is used to select the devices for this object and enable VPN connections. The Users tab is used to select which users can connect to this system over the incoming connection object. Furthermore, you can select "Require all users to secure their passwords and data" and whether to allow directly connected devices to connect without providing a password. By opening the Properties for a specific user, you can change that user's full name and password and set the callback options. The Networking tab is where the networking components are enabled and configured.

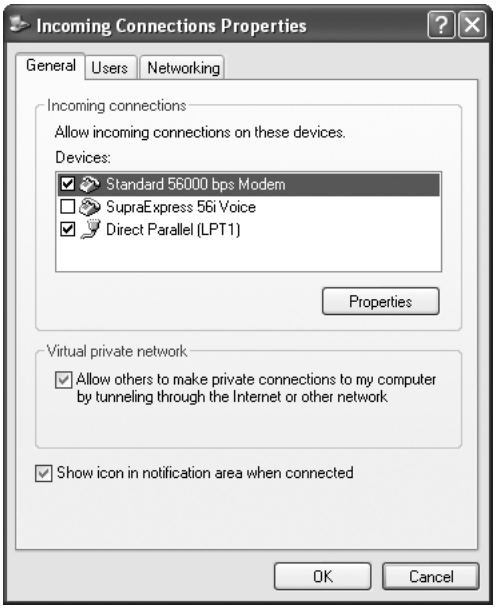

Figure 8-11 An Incoming Connections Properties dialog box, General tab

Once an incoming connection object is created, the devices selected for that object are placed in answer mode. When a call is received by that device, Windows XP automatically answers the call and attempts to authenticate the connection. When a device is placed into answer mode, it can only be used by one process for incoming connections, but such a device can be used to establish outbound calls. In other words, creating an incoming connection object for your modem won't prevent you from using that modem to establish a connection with your ISP or office LAN. However, it does prevent you from running two answering processes at the same time, such as remote access and fax.

Connecting Directly to Another Computer

All too often, you'll discover that you need to move several MB of data from one system to another when one or both of the systems has no network interface. In such cases you have only a few reasonable options: use a floppy spanning tool, purchase and install a NIC, purchase and install removable media devices (such as Zip drives), or create a direct cable connection. Obviously, spanning floppies is often a doomed task, especially when working with more than 3 MB of material. If you had the budget for a NIC or a removable media device, you probably would have them installed already. The best option is to use a serial or parallel cable (or even infrared port if already present on both systems), directly connecting the computers, which you probably already have on hand or can purchase one for less than $10.

To employ the direct connection, first attach the cable (or orient the infrared devices) between the two systems. Next, you'll need to create a direct connection object on both

systems; one acts as the host and the other acts as the guest. Just be sure to select the correct link type based on your hardware (i.e., serial, parallel, or infrared). To create the direct connection objects, follow the steps in Hands-on Project 8-5.

You can create the host connection object through either the Accept incoming connections or the Connect directly to another computer Wizard suboptions of the Set up an advanced connection option. But you can create the guest or connecting object only through the Connect directly to another computer Wizard option.

Once the link is established, you'll have the same link to the other system as if you were both members of the same workgroup connected by normal network cables.

The Properties dialog box for a host direct connection object is the same as that of an incoming connection object. The Properties dialog box for a guest connection object is the same as that of any dial-out connection object, with the General tab offering control over the connection device.

Installing Remote Access Hardware

Before any remote access connection can be established, the hardware required by that connection must be physically present and its drivers properly installed. Under Windows XP, the process of installing hardware is often simple and requires little user input. Upon boot-up, Windows XP inspects the hardware and attempts to identify any new devices. If a device is recognized, Windows XP attempts to locate and install drivers for it. In some cases, you'll be prompted for additional paths to search for drivers. When Windows XP is unable to identify a device, you'll either be prompted to provide a path for the drivers or you'll need to use the Add/Remove Hardware applet or the Phone and Modem Options applet to install the drivers. For some specialty hardware, such as cable modems and DSL devices, you might need to use the vendor-supplied installation routine to install the correct drivers.

Because of the wide range of remote access-related devices, we recommend consulting the device's manual or contacting the vendor for further aid with installation; this will be necessary only for a few uncommon devices.

Phone and Modem Options

The primary Control Panel applet for remote access devices and operations is Phone and Modem Options, which is used to control dialing rules, modems, and telephony driver properties. The Dialing Rules tab lists the defined dialing location, a collection of remote access properties used to govern how links are established. This tab offers the controls of New (to create new locations), Edit (to alter existing locations), and Delete

(to remove a location). Both New and Edit open the same three-tabbed interface where the default or existing settings for a location can be altered.

The General tab of a New Location (see Figure 8-12) is used to define the following:

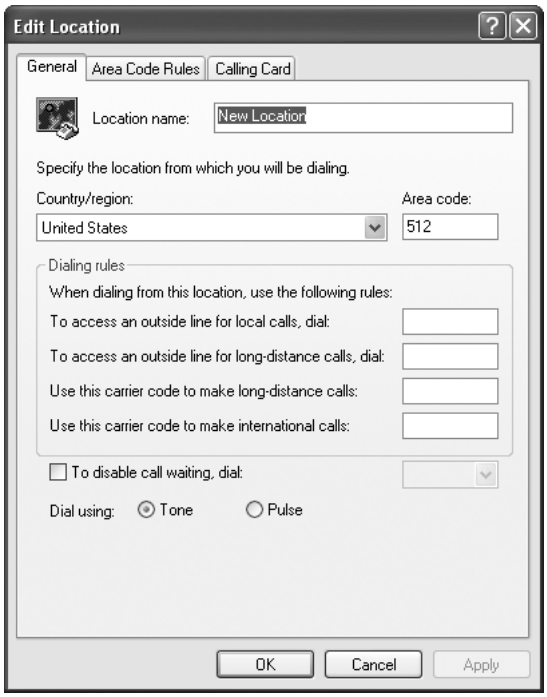

Figure 8-12 The Edit Location dialog box, General tab

- Location name
- Country/region
- Area code
- Number to dial to gain access to an outside line for local calls
- Number to dial to gain access to an outside line for long distance calls
- Use this carrier code to make long-distance calls
- Use this carrier code to make international calls
- Disabling call waiting
- Dial using pulse or tone

The Area Code Rules tab is used to define how numbers that exist within or outside of the current area code are dialed. These rules include which prefixes (the first three numbers of

a seven-digit phone number) are included in an area code (and thus are local calls), whether to dial 1 (one) first when calling certain prefixes, and whether to include the area code when dialing certain prefixes.

The Calling Card tab is used to specify a method for charging long distance calls to a credit card or dialing card. There are dozens of predefined cards that require you to provide only your account number and PIN, or you can define your own calling card billing rule. Consult the online help and the *Microsoft Windows XP Professional Resource Kit* for details on calling card rule creation.

Once you've created an alternate location by setting the dialing rules, that location appears in a pull-down list on most connection object connect interfaces. You can select the location profile to use each time you initiate a remote access link.

The Modems tab of the Phone and Modem Options applet lists all currently installed modems and their attached ports. New modems are installed by clicking the Add button; existing modems can be deleted with the Remove button. The Properties button is used to access device/driver specific properties and configuration controls.

The Advanced tab of the Phone and Modem Options applet lists all the telephony providers present on the system. These are the drivers employed by the remote access system to link communication devices and networking components. Telephony providers are the interface between the operating system and the communication device. In most cases you'll never use this tab. Consult the *Microsoft Windows XP Professional Resource Kit* or the telephone provider's vendor for configuration information.

Remote Access Security

Remote access security is built on Windows XP's local and network security. A remote access connection is simply another type of network connection. This means that remote users still must pass log-on authentication and have the correct user/group permissions to gain access to shared resources. However, remote access boasts several additional security measures to aid in keeping break-ins and unauthorized access to a minimum. Remote access connections can be protected from unwanted traffic by using the Internet Connection Firewall (discussed later in this chapter).

Dial-up connection objects have authentication and encryption security options. These are defined on the Security tab of their Properties dialog box, and were discussed earlier in the Connect to the Internet section. Basically, they define whether a password can be transmitted in clear text (i.e., without encryption) or requires encryption, what encryption methods can be used, whether data encryption is required, and whether a smart card is required.

Remote access does not restrict the ability to dial out from a Windows system. As long as there is a modem and a defined connection object, any user of the system can initiate a dial-out connection. However, there is a strict limitation on who can dial into a

Windows system. As discussed earlier in regard to accepting incoming connections, only selected users will be authorized to connect when they attempt to dial-in. For each user that is granted dial-in access, you can also define callback security. Furthermore, the incoming connection can require that all passwords and data be secured with encryption.

In addition to these security controls, remote access can be further secured using a VPN protocol. Whether the Internet is involved or not, PPTP or L2TP can be used to establish a secured and encrypted communication pipeline between the client and answering system. L2TP offers encryption using IPSec or IP Security. For more information on IPSec, see the "IP Security Policies" section of Chapter 6, "Windows XP Security and Access Controls."

Internet Options Applet

The Internet Options applet (see Figure 8-13) is used to define settings for Internet Explorer and general Internet access. This applet has seven tabs. The General tab sets the home page, temporary file cache, URL history, colors, fonts, languages, and accessibility options. The Security tab defines the security level for four Web zones. The security level determines whether software is automatically downloaded, form data is submitted, or cookies (text scripts that a Web browser sends to a server to customize a user's browsing experience) are used. The Privacy tab is used to set the level of personal information that is shared or restricted when communicating with a Web site. The Content tab is used to configure the Content Advisor (a content-based site blocker), identity certificates, AutoComplete, and your online identity. The Connections tab is used to define how IE (Internet Explorer) and other online tools access the Internet through a LAN or dial-up network connection, which is often used for home Internet service connections. The Programs tab is used to specify which helper applications are used for HTML editing, e-mail, newsgroups, Internet calls, calendar, and contacts. The Advanced tab is used to set advanced features, such as browsing functions, HTTP 1.1, multimedia, printing, searching, security, and accessibility.

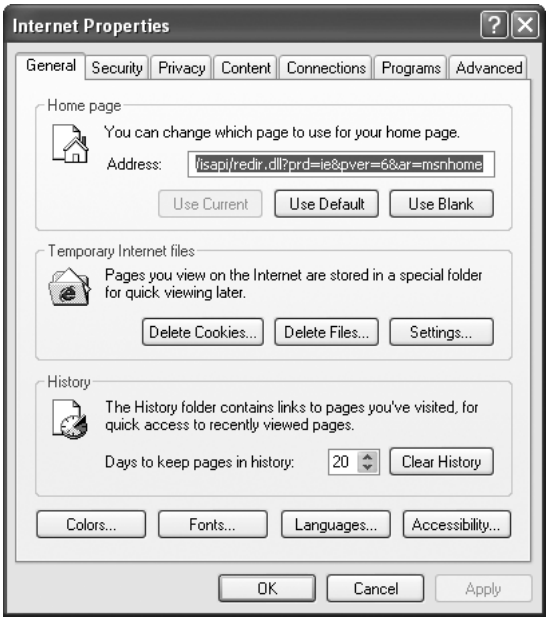

Figure 8-13 Internet Options applet

The four Web zones controlled on the Security tab are Internet, Local intranet, Trusted sites, and Restricted sites. Each zone can have a predefined default level or a customized level of security restrictions placed on that zone. The predefined default security levels are High, Medium, Medium-low, and Low. The security restrictions for each of these are as follows:

- *Low*—Provides minimal safeguards and warning prompts, most content is downloaded and run without prompts, all active content can run, and appropriate for sites that you absolutely trust. This is the default security level of the Trusted sites zone.
- *Medium-low*—Same as Medium without prompts, most content will be run without prompts, unsigned ActriveX controls will not be downloaded, and appropriate for sites on your local network (intranet). This is the default security level of the Local Intranet zone.
- *Medium*—Provides for safe browsing and still is functional, prompts before downloading potentially unsafe content, unsigned ActiveX controls will not be downloaded, and appropriate for most Internet sites. This is the default security level of the Internet zone.

- *High*—This is the safest way to browse, but also the least functional. Less secure features are disabled, and appropriate for sites that might have harmful content. This is the default security level of the Restricted zone.

The content of this bulleted list is taken directly from the Security tab of the Internet Options dialog box of Windows XP Professional. Copyright is held by Microsoft.

These restrictions can include controls set for Disable, Enable, or Prompt (or possible custom settings based on security control) over downloading signed ActiveX controls, downloading unsigned ActiveX controls, run ActiveX scripts not marked as safe, run ActiveX controls and plug-ins, run ActiveX scripts marked as safe, file downloads, font downloads, Java permissions, etc.

The Internet zone contains all sites on the Internet or local intranet that have not been placed in any of the three other zones. The Local intranet zone contains those sites within your local intranet. This list is created automatically based on include/exclude selections of three controls: all local sites not in other zones, all sites that bypass the proxy server, and all network UNC paths. The Trusted sites zone includes only those sites that you add to this zone specifically. You should only add sites to this zone that you highly trust. You can force https server verification for all sites in this zone. The Restricted zone includes only those sites that you specifically add to this zone. You should add any site you discover that attempts to cause harm.

The Content Advisor—accessed from the Content tab of the Internet Options dialog box—is used to control site access based on RSACi content ratings. You are able to select the level of language, nudity, sex, and violence which users are allowed to see. Pre-approved sites can be defined using the site's URL as always accessible or never accessible. You can allow users to view all non-rated sites; however, this option is disabled by default. You can also define a supervisor password that allows access to all previously restricted content.

For details on configuring Internet Explorer, consult the IE Help file or the IE Web site at *http://www.microsoft.com/windows/ie/default.htm.*

Internet Connection Sharing

Internet Connection Sharing (ICS) is used to share a single network connection with a small group of networked computers. The shared connection can be a link to the Internet or any type of network. ICS is enabled on the Advanced tab of a connection object's Properties dialog box (refer to Figure 8-10 earlier in the chapter). By enabling sharing for a connection object, you allow other computers on your network to access resources over that external link.

Internet Connection Sharing incorporates the Network Address Translation (NAT) function, a Dynamic Host Configuration Protocol (DHCP) address allocator, and a Domain

Name Service (DNS) proxy. The mechanism hides your internal network configuration (keeping this information secure), provides automatic assignment of unregistered non-routable IP addresses to internal clients, and provides a forwarding hand-off procedure for all requests for external services. Basically, Internet Connection Sharing transforms your Windows XP system into a limited DHCP proxy server. After ICS is enabled, you must set all other clients to use DHCP in order to take advantage of the shared connection. Try Hands-on Project 8-8 to configure Internet Connection Sharing.

Once Internet Connection Sharing is enabled, you can also select whether to enable on-demand dialing. This feature automatically re-establishes the remote link when a client attempts to access external resources over your system through the currently offline connection object. Microsoft recommends using ICF on each ICS link for added security. For further tuning and configuration of the Internet Connection Sharing service, consult the *Microsoft Windows XP Professional Resource Kit*.

Troubleshooting the Internet Connection Service involves two distinct activities. First, verification that the connection is active and functioning can usually be accomplished using a Web browser. Second, verification that communication from other clients can access your system over the network can be achieved either by pinging or by attempting to access a shared resource from your client.

Once ICS is enabled, you can also define which services running on your internal network are accessible to external Internet users. This is performed through the Settings button on the Advanced tab, which opens the Advanced Settings dialog box. If you have enabled only ICS, then the Advanced Settings dialog box has a single tab—Services. However, if you have enabled ICF, then this dialog box has three tabs (discussed in the ICF section, see Figure 8-14). Windows XP is configured by default to allow access to L2TP, PPTP, and IKE (i.e., IPSec) resources. This allows external VPN clients to establish a connection into the network over the dial-up link. If you want to share other resources, you can enable FTP, IMAP, SMTP, POP, Remote Desktop, HTTP, Telnet, and HTTP. Other services can be defined by using the Add or Edit buttons.

ICS should not be used on any network with domain controllers, DNS servers, gateway systems, DHCP servers, or with clients that must have static IP addresses. ICS is designed for use on small workgroup networks, not within domains. ICS and normal DHCP interfere with each other. ICS uses the 192.168.x.x network to assign IP addresses to clients and does not support statically configured clients. For sharing an Internet connection with a domain, use the proxy routing and NAT capabilities of a Windows Server product.

Internet Connection Firewall

The Internet Connection Firewall (ICF) is a security measure for protecting network connections from unwanted traffic. ICF can set restrictions on traffic in and out of your network to an external network or the Internet. Microsoft recommends that ICF be used on each ICS link, but ICF can be used on LAN connections as well. In fact, Microsoft

recommends using ICF on every network connection to an external network except those that host VPN links. ICF is a much needed feature for systems that employ shared broadband connections, such as cable modems or even campus networks. On shared broadband connections, the potential exists for one client customer to infiltrate another client's system. Only a secure personal firewall can prevent such infiltration.

ICF is a stateful firewall, which means each packet that passes ICF is inspected to determine its source and destination addresses. This allows ICF to prevent any external traffic not requested by an internal client from entering the private network. However, ICF can also be configured to allow specific types of traffic to enter the private network without a corresponding internal client request. These features are defined on the Services tab of the Advanced Settings dialog box (see Figure 8-14) accessed through the Settings button on the Advanced tab of a connection object's Properties dialog box (as discussed in the section of this chapter on ICS).

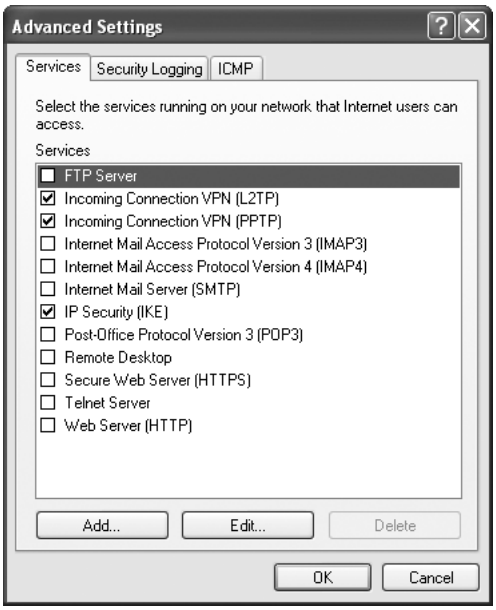

Figure 8-14 Advanced Settings dialog box, General tab.

By default, ICF silently drops all traffic that is not allowed to enter the private network. In other words, it does not record a log file of dropped packets. If you want a record of dropped packets or successful connections, logging can be enabled on the Security

Logging tab. You can use the logging ICF actions to determine which ports or services outside are attempting to connect to and which are succeeding. You might find some surprising footprints in the logs. Such as finding out that you have a Web server running on the default port 80 and some external user is regularly connecting to it. Rogue connections into your system, whether over a LAN or Internet connection can significantly reduce the performance of your system and compromise your security.

The ICMP tab is used to configure to which external system ICMP requests the ICF-protected system will respond.

Try Hands-on Project 8-9 to configure Internet Connection Sharing.

Windows XP and the Internet

Windows XP Professional features a number of tools to help you access the vast resources of the Internet: Internet Explorer, Outlook Express, FTP client, Telnet client, and Internet Information Server (IIS), Connections can be established through Network Connections to the Internet or an Internet access point (such as a LAN with a proxy server).

Internet Explorer

Microsoft's Internet Explorer (IE) version 6.0 is included with the Windows XP operating system (this was the current release of IE when Windows XP was developed). Newer versions of IE can be obtained from the Microsoft Web site at *http://www.microsoft.com/ie/*.

IE is a state-of-the-art Web browser. In addition to being powerful and easy to use as a Web-surfing tool, IE is tightly integrated with other Windows applications; it can invoke Word to open .doc files or Excel to open .xls files across the Web. The program also includes advanced support for newsgroups and FTP and is tightly integrated with Outlook Express.

Outlook Express

One of the most popular e-mail client utilities is Outlook, a part of the suite of applications known as Microsoft Office. To tempt you with its impressive features and offer you a taste of a multi-function e-mail client, Microsoft has included Outlook Express in Windows XP. Outlook Express is limited only by the types of messaging it supports—it can manage only Internet e-mail involving POP3, IMAP, and SMTP services. Outlook Express can be used to read and write e-mail, file and sort messages, and more. It can act as a contact management tool, is integrated with IE for easy task switching, and offers customizable interfaces and rules (actions to be performed on messages automatically).

If "free" is your first criterion when choosing an e-mail package, Outlook Express is no slouch. However, if you are not above spending a few dollars for a worthwhile product, Outlook is worth the upgrade. For more information on Outlook and Outlook Express, visit *http://www.microsoft.com/outlook/*.

FTP Client

As mentioned earlier, FTP is an IP-based Application layer protocol that handles file transfer and remote file system access and manipulation functions. Microsoft includes a command-line implementation of an FTP client as part of the Windows XP operating system. This client is installed automatically when TCP/IP is installed.

To learn more about this program, launch a DOS window (Start|All Programs|Accessories|Command Prompt) and enter *ftp* at the command line. When the ftp> prompt appears, enter *help* to read the program's associated list of commands (enter *help <command>* to obtain information about a specific command, where you replace *<command>* with the name of an actual FTP command, like *get* or *put*).

Even though the command-line version of FTP included with Windows XP is perfectly adequate, there are numerous freeware and shareware GUI implementations of FTP that can take its place and are much easier and friendlier to use. For a complete listing of such utilities, visit either of these Web sites, select Windows as the platform, and use "FTP" or "FTP client" as your search string:

- *http://www.shareware.com*
- *http://www.download.com*

The authors are quite partial to the IpSwitch package, WS_FTP Professional. It combines an Explorer-like file interface with easy controls for uploads and downloads. Visit *http://www.ipswitch.com/* to download an evaluation version.

Telnet Client

Telnet is the text-based remote interaction tool commonly used on older UNIX systems to gain access to shell accounts. Some ISPs still offer shell access to customers. The Telnet client included with Windows XP is a simple tool that attempts to establish a Telnet session with a remote system based on domain name or IP address. You can alter the display fonts and record the session for later perusal (it's all text anyway). For more information on Telnet, type telnet at a Command Prompt (Start | All Programs | Accessories | Command Prompt), then select Contents from the Help menu of the Telnet window.

Internet Information Server

A reduced functionality version of Internet Information Server (IIS) is included with Windows XP Professional to allow a system to host Web and FTP services. In most cases, IIS on a client system (such as Windows XP Professional) is used for site development and testing before deployment on an IIS system (such as Windows NT Server, Windows 2000 Server, or Windows .NET Server). When hosted by Windows XP Professional, IIS is limited to the same 10 simultaneous connections as Windows XP Professional itself. Thus, it is not a platform designed or intended for public Web/FTP site hosting.

Perhaps the most important and widely recognized function of IIS is the WWW (World Wide Web) Service. This service allows the user to publish Hypertext Markup Language (HTML) documents for use on the Web. Web browsers like Internet Explorer use the Hypertext Transfer Protocol (HTTP) to retrieve HTML documents from servers.

Overlooking limitations on the number of simultaneous users and the omission of certain site management tools, the two environments (IIS on Windows XP Professional and IIS on a Windows Server) are nearly identical. Certainly they're adequate to facilitate Web site development on a Windows XP Professional system with IIS, for ultimate deployment on Windows Server system with IIS.

The FTP Server installed with IIS is used to transfer files from the server to remote computers. Most installations of FTP on the Internet are used to download drivers and other data or software files.

This code module represents the server side of FTP, whereas the software mentioned earlier in the chapter covered the client side of FTP. In other words, this module permits machines elsewhere on the network to upload files to or download files from an Windows XP Professional system. The client-side software only permits the system to perform the same activities with other FTP servers elsewhere on the network.

Web server resources are managed similarly to any other network resource. You should think of Web and FTP services as a type of share for Internet clients. Thus, troubleshooting Web resource access problems is like troubleshooting typical network shared resource access problems. You need to manage file permissions on an NTFS file object level and general access to resources through the share (or in this case Web or FTP services). If a user is unable to gain access to a resource through the Web or FTP, check the NTFS file object-level permissions first on the file/object/resource itself, then on all of its parent containers. Next, check the setting on the Web or FTP service itself. To access resources over Web or FTP, the user must have at least Read access granted through the service and at least Read access on the file or resource based on group memberships. Keep in mind that most Web access is anonymous, whereas many FTP sites require user authentication for access. However, the logon credentials for FTP are transmitted in clear text. The anonymous user account IUSR_<computername> is a member of the Everyone and the Authenticated Users groups. This account is used to "authenticate" anonymous users on both Web and FTP sites hosted by IIS. Be sure to check the permissions for these groups as well.

A single Windows XP Professional system (or any Windows NT or 2000 system) can be assigned multiple IP addresses. When a system has multiple IP addresses and is the host of IIS as a Web server, each Web site can be assigned its own IP address. Assigning each Web site a different IP address is handled on the Web Site tab of the Properties dialog box. Just set the IP Address field to the specific IP address you want this Web site to use.

If you want to host multiple Web sites from a system that has only a single IP address, you must employ host headers. Host headers are defined through the Advanced button

located alongside the IP Address field on the Web Site tab of the Properties dialog box of a Web site. Each unique Web site should be assigned its own host header. A host header is usually a word, short phrase, domain name, or title that the administrator of the Web site wants to use as the distinguishing element for that site. The host header is never seen by the Web user. If host headers are not used, a Web user would always see the first or default Web site hosted by the one-IP address IIS Web server even if they used the URL or domain name of any other Web site hosted by that Web server.

For more information on IIS, consult the *Microsoft Windows XP Professional Resource Kit* or the *Microsoft Windows .NET Server Resource Kit*.

Order Prints Online

Order Prints Online is a feature of the My Pictures folder and any media folder defined as an image repository (see the "Media Folders and the Customize Tab" section in Chapter 4, "Managing Windows XP File System and Storage"). This command launches the Online Print Ordering Wizard, which walks you through the process of submitting digital images to a printing company. You'll select the images to print, the sizes, quantities, and billing and shipping information. The Wizard requires that Internet access be available. If you need help with the Wizard, use the Help and Support Center of Windows XP.

Clients vs. Server-Based Remote Access

Choosing which platform to use as a remote access server is usually straightforward. Windows XP Professional is limited to a single incoming dial-up connection and can support only 10 simultaneous network connections (including LAN and VPN). Windows 2000 Server and Windows .NET Server both support up to 256 concurrent incoming dial-up connections and have no hard restriction on number of simultaneous network connections (restricted by license for LAN and hardware for VPN or Internet connections). Windows XP Professional can share an Internet link with a workgroup, but the workgroup is forced to use DHCP, and the range of IP addresses is assigned by ICS. Windows Servers offer Internet connection sharing through a proxy router that does not restrict the clients to DHCP or a specified IP address range. Windows XP Professional lacks a full-featured version of IIS, which is integrated into Windows Server products.

From these issues, it is clear that a small workgroup network can use Windows XP Professional as its remote access server if it can operate within the connection limitations. If an organization requires greater flexibility and connectivity, a Windows Server should be selected to act as the remote access server.

Remote Access Troubleshooting

Remote access problems can be fairly elusive, but there are several common-sense first steps and several useful Windows XP tools to simplify the process of troubleshooting. Your first approach to a remote access problem should include considerations for:

- Physical connections (phone lines, serial cables, etc.)
- Power to external devices
- Properly installed and updated drivers
- Properly configured settings
- Correct authentication credentials
- Similar encryption or security requirements
- Proper protocol requirements and settings

If reviewing these items still fails to uncover the problem, there are several log files you can examine to hopefully glean more specific information. There are three logs related to remote access events. The first log is a file containing all communications made between the OS and the modem device during connection establishment. This log must be enabled through the Diagnostics tab of the modem's Properties on the Modems tab of the Phone and Modem Options applet. Once enabled, a text file named after the modem (in the format "ModemLog_Practical Peripherals PC288LCD V.34.txt") is stored in the main Windows XP directory. This file can be viewed with Notepad or simply by clicking View Log next to the enable checkbox on the Diagnostics tab.

The second log file, PPP.LOG, records the communications involved in the setup, management, and continuity of a PPP connection. This log is enabled by editing the Registry. The PPP value in the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\ key should be set to 1 to start the logging. This file is stored in the %systemroot%\tracing folder.

The final log is the System log as viewed through the Event Viewer. This log often records events related to remote access connection failures.

By combining data gleaned from these logs, you should be able to determine the cause of your connection problem and easily discover a simple resolution. If you need further remote access troubleshooting help, consult the *Microsoft Windows XP Professional Resource Kit*.

Chapter Summary

- In this chapter, we've introduced you to the Windows XP Remote Access Service, including the significant features of remote access in Windows XP. We've examined

remote access WAN connections and protocols, how to install and configure remote access, and how take full advantage of remote access dial-up networking and security features. With all this information, you should be ready to dial into your Windows XP Professional system from the outside or use it to dial out to a service provider. Additionally, we discussed the Internet access features built into Windows XP and how they can be employed to gain access to vast public and private resources. Windows XP is also designed to participate in virtual private networks (VPNs) by establishing an encrypted link between two systems over the Internet.

KEY TERMS

Dynamic Host Configuration Protocol (DHCP) — A method of automatically assigning IP addresses to client computers on a network.

gateway — A computer that serves as a router, a format translator, or a security filter for an entire network.

Integrated Services Digital Network (ISDN) — A direct, digital dial-up PSTN Data Link-layer connection that operates at 64KB per channel over regular twisted-pair cable between a subscriber site and a PSTN central office.

Layer Two Tunneling Protocol (L2TP) — A VPN protocol developed by Cisco Systems, Inc. to improve security over Internet links by integrating with IPSec.

modem (modulator/demodulator) — A Data-link layer device used to create an analog signal suitable for transmission over telephone lines from a digital data stream. Modern modems also include a command set to negotiate connections and data rates with remote modems and to set their default behavior.

Point-to-Point Protocol (PPP) — A Network layer transport that provides connectivity over serial or modem lines. PPP can negotiate any transport protocol used by both systems involved in the link and can automatically assign IP, DNS, and gateway addresses when used with TCP/IP.

Point-to-Point Tunneling Protocol (PPTP) — Protocol used to connect to private networks through the Internet or an ISP.

port — Any physical communication channel to which a modem, direct cable, or other device can be connected to enable a link between two computers.

PPP MultiLink — A capability of remote access to aggregate multiple data streams into one network connection for the purpose of using more than one modem or ISDN channel in a single connection.

Public Switched Telephone Networks (PSTN) — A global network of interconnected digital and analog communication links originally designed to support voice communication between any two points in the world, but quickly adapted to handle digital data traffic.

Remote Access Service (remote access) — The service in Windows XP that allows users to log into the system remotely.

serial — A method of communication that transfers data across a medium one bit at a time, usually adding start and stop bits to ensure reliable delivery.

Serial Line Internet Protocol (SLIP) — An implementation of the IP protocol over serial lines. SLIP has been made obsolete by PPP.

wide area network (WAN) — A geographically dispersed network of networks connected by routers and communications links. The Internet is the largest WAN.

X.25 — A standard that defines packet switching networks.

Review Questions

1. You have configured a Windows XP Professional client to dial up and establish a connection to a Windows Server computer. The user adds a dial-up connection object, sets the proper network configuration, and the modem is functioning properly. The user submits the user name and password correctly. Unfortunately, the user is unable to authenticate properly. What might be causing this problem?
   a. The user did not configure the gateway properly.
   b. The user was not granted the appropriate dial-in permissions.
   c. The user was not added to the dial-in users group.
   d. Internet Connection Firewall was blocking the authentication
2. DHCP is the option for automatically assigning IP configuration to TCP/IP dial-up clients. True or False?
3. Windows XP Professional supports PPP logon scripts. True or False?
4. Which of the following remote access-related logs are enabled by default?
   a. PPP.LOG
   b. Modemlog_<modem name>.txt
   c. System log
5. Which of the following encrypted authentication options does Windows XP Professional support through remote access? (Choose all that apply.)
   a. PAP
   b. SPAP
   c. DES-3
   d. MS-CHAP
   e. PGP
6. The special protocol _____ allows multiple channels to be aggregated to increase bandwidth.
   a. Multilink PPP
   b. PPTP
   c. PPP
   d. SLIP

7. Where in Windows XP Professional do you specify which users have dial-in permissions to the remote access server?
   a. Network Connections
   b. Control Panel
   c. Remote Access Admin Tool
   d. My Computer
8. Which remote access security option also has an additional option to encrypt data?
   a. Require encrypted authentication
   b. Require C2 encrypted authentication
   c. Require B encrypted authentication
   d. Require Microsoft Encrypted Authentication
9. Which remote access callback option provides the greatest level of security?
   a. Set by Caller
   b. Set by Server
   c. Preset to
   d. Callback and confirm remote access password.
10. Which of the following protocols are supported by both Windows XP remote access clients and servers?
    a. SLIP
    b. PPP
    c. none of the above
    d. all of the above
11. Which of the following are similar technologies used to establish secured WAN links over the Internet?
    a. MPPP
    b. PPTP
    c. SLIP
    d. L2TP
12. Help-U-Sell has just opened a new office in Cedar Park, TX. They have a small workgroup network of eight computers. A cable modem has been installed. Which of the following technologies should be used to provide each system in the office with Internet access and prevent as much unwanted traffic as possible?
    a. IPSec
    b. ICS
    c. ICF
    d. Callback
    e. L2TP

13. Which connection protocol can be used by Windows XP Professional to connect to remote systems over standard telephone lines?
    a. SLIP
    b. PPP
    c. DLC
    d. PPTP
14. By default, Internet Connection Firewall blocks traffic of which service type if it originates from the Internet instead of responding to a request by an internal client?
    a. FTP
    b. L2TP
    c. POP3
    d. IKE
    e. Remote Desktop
    f. Telnet
    g. HTTP
15. The Create a new connection Wizard from Network Connections is used to create both remote access connections and standard LAN connections. True or False?
16. If you want to connect only to servers that offer secured data transmission, which of the following encryption settings should you define for your connection object?
    a. No encryption allowed (server disconnects if it requires encryption)
    b. Optional encryption (connect even if no encryption)
    c. Require encryption (disconnect if sever declines)
17. Windows XP supports Direct Cable Connections under remote access using:
    a. RS-232 Null Modem Cables
    b. APC UPS Cables
    c. LapLink Cables (i.e. parallel pass-through cables)
    d. Printer Cables
18. Remote access is remote control for Windows XP. True or False?
19. Internet Connection Sharing can be used to share which of the following types of connections with a workgroup network?
    a. Internet
    b. LAN dial-up
    c. VPN
    d. Incoming
    e. Bridge connection

20. You can connect to another computer from a remote access client using resources in the same manner as if you were connected on a LAN. True or False?
21. Dialing rules or Dialing locations are used to define the geographic location of a mobile computer so as to prescribe the dialing procedures. True or False?
22. The modem specific log file is enabled through what utility?
    a. Computer Management
    b. Phone and Modem Options
    c. Network Connections
    d. Server applet
23. Which of the following are Internet utilities included with Windows XP Professional?
    a. Internet Explorer
    b. Internet Information Server
    c. Outlook
    d. Telnet
    e. FTP client
24. In which of the following situations would the use of Windows XP Professional as a remote access server be a reasonable option?
    a. A single telecommuter needs to connect into the office network
    b. A domain network needs Internet access
    c. A SOHO network needs Internet access
    d. A high-traffic e-commerce Web site needs hosting
    e. A private network needs internal Web documentation access
25. Offline Files are cached locally at logoff, are accessed in the same way as the original files, and are automatically synchronized by default. True or False?

HANDS-ON PROJECTS

Project 8-1

To create a Dial-up connection object to a private network:

This hands-on project assumes that a modem is installed. You need the phone number of a remote access server to contact. If this lab is to be used as a demonstration only, use 555-1212 as the phone number.

1. Open the Control Panel (**Start**|**Control Panel**).

2. Click **Switch to Classic View** if the Control Panel is currently in Category View.
3. Double-click **Network Connections**.
4. Launch the New Connection Wizard by double-clicking the **Create a new connection** link in the Quick List.
5. The first page of the Wizard is a welcome message. Click **Next**.
6. On the Network Connection Type page, select **Connect to the network at my workplace**. Click **Next**.
7. On the Network Connection page, select **Dial-up connection**. Click **Next**.
8. If you have two or more dial-up devices installed on your system, you will see the Select a Device page. Otherwise, skip to step 9. On the Select a Device page, select the communication device(s) for this connection object. Devices with a marked checkbox are used by this object; devices with an empty checkbox are not. If you select multiple devices, the system attempts to aggregate the links through multilink. Click **Next**.
9. On the Connection Name page, provide a name for this connection object such as **HoP 8-1**. Click **Next**.
10. On the Phone Number to Dial page, provide the dial-up number for your remote access server. Click **Next**.
11. On the Connection Availability page, select whether this connection will be available for Anyone's use or My use only. Click **Next**.
12. Click **Finish**. The Create a new connection Wizard completes the connection object creation (i.e., it now appears in the Network Connections window), but instead of returning you to the Network Connection window, the Wizard launches the new connection object for the first time.
13. On the Connect dialog box, provide the name of the user account to employ when connecting to the remote access system.
14. In the Password field, type the password for that user account. Your keystrokes will be echoed with asterisks instead of the actual character you typed to prevent over-the-shoulder theft of your password.
15. If you want the system to retain your password, select **Save this user name and password for the following users:**, then select Me only or Anyone who uses this computer. If you decide not to check this box, you'll have to provide the password each time this connection object is used to establish the remote access link.
16. Double-check that the listed phone number in the Dial field is correct. If not, change it to the correct number.
17. To initiate the connection, click **Dial**. If this project is being performed as an example rather than a real-life implementation, skip this step.

Project 8-2

To create a dial-up connection object to connect to an ISP:

This hands-on project assumes that a modem is installed. This lab performs a manual ISP configuration, which requires a phone number and valid username and password. If this lab is to be used as a demonstration only, use 555-1212 as the phone number.

1. Open the Control Panel (**Start|Control Panel**). Click **Switch to Classic View** if the Control Panel is currently in Category View.
2. Double-click **Network Connections**.
3. Launch the New connection Wizard by double-clicking the **Create a new connection** link in the Quick List.
4. The first page of the Wizard is a welcome message. Click **Next**.
5. On the Network Connection Type page, select **Connect to the Internet**. Click **Next**.
6. On the Getting Ready page, select **Set up my connection manually**. Click **Next**.
7. On the Internet Connection page, select **Connect using a dial-up modem**. Click **Next**.
8. If you have two or more dial-up devices installed on your system, you will see the Select a Device page. Otherwise, skip to step 9. On the Select a Device page, select the communication device(s) for this connection object. Devices with a marked checkbox will be used by this object; devices with an empty checkbox will not. If you select multiple devices, the system will attempt to aggregate the links through multilink. Click **Next**.
9. On the Connection Name page, provide a name for this connection object, such as **Lab ISP1**. Click **Next**
10. On the Phone Number to Dial page, provide the dial-up number for your ISP. Click **Next**.
11. On the Connection Availability page, select whether this connection will be available for Anyone's use or My use only. Click **Next**.
12. On the Internet Account Information page, provide the username and password for the ISP account.
13. By default, the selections of Use this account name and password when anyone connects to the Internet from this computer, Make this the default Internet connection, and Turn on Internet Connection Firewall for this connection are marked. If this is acceptable, click **Next**.
14. Click **Finish**. The Create a new connection Wizard completes the connection object creation (i.e., it now appears in the Network Connections window), but instead of returning you to the Network Connections window, the Wizard launches the new connection object for the first time.

15. On the Connect dialog box, double-check the name of the user account you need to employ when connecting to the ISP.
16. If you want the system to retain your password, select the **Save this user name and password for the following users:** checkbox, then select Me only or Anyone who uses this computer. If you decide not to check this box, you'll have to provide the password each time this connection object is used to establish the remote access link.
17. Double-check that the listed phone number in the Dial field is correct. If not, change it to the correct number.
18. To initiate the connection, click **Dial**. If this project is being performed as an example rather than a real-life implementation, skip this step.

Project 8-3

To create a VPN connection object:

This hands-on project performs a VPN configuration, which requires a host name or IP address of the remote system to connect to. If this lab is to be used as a demonstration only, use 172.16.1.1 as the IP address of the remote system.

1. Open the Control Panel (**Start**|**Control Panel**). Click **Switch to Classic View** if the Control Panel is currently in Category View.
2. Double-click **Network Connections**.
3. Launch the New Connection Wizard by double-clicking the **Create a new connection** link in the Quick List.
4. The first page of the Wizard is a welcome message. Click **Next**.
5. On the Network Connection Type page, select **Connect to the network at my workplace**. Click **Next**.
6. On the Network Connection page, select **Virtual Private Network connection**. Click **Next**.
7. On the Connection Name page, provide a name for this connection object, such as **Lab VPN 1**. Click **Next.**
8. On the Public Network page, select **Do not dial the initial connection**. If you want this VPN connection to establish an Internet connection automatically before initiating the VPN link, then select **Automatically dial this initial connection** and make a choice from the pull-down list. Click **Next**.
9. On the VPN Server Selection page, provide the host name or IP address of the remote system to connect to. Click **Next.**

10. On the Connection Availability page, select whether this connection will be available for Anyone's use or My use only. Click **Next.**
11. Click **Finish**. The Create a new connection Wizard completes the connection object creation (i.e., it now appears in the Network Connections window), but instead of returning you to the Network Connections window, the Wizard launches the new connection object for the first time.
12. On the Connect dialog box, provide the username and password needed to authenticate to the remote system.
13. If you want the system to retain your password, select the **Save this user name and password for the following users:** checkbox, then select Me only or Anyone who uses this computer. If you decide not to check this box, you'll have to provide the password each time this connection object is used to establish the remote access link.
14. To initiate the connection, click Dial. If this project is being performed as an example rather than a real-life implementation, skip this step.

Project 8-4

To create an Incoming connection object:

This hands-on project assumes that a modem is installed.

1. Open the Control Panel (**Start|Control Panel**). Click **Switch to Classic View** if the Control Panel is currently in Category View.
2. Double-click **Network Connections**.
3. Launch the New Connection Wizard by double-clicking the **Create a new connection** link in the Quick List.
4. The first page of the Wizard is a welcome message. Click **Next**.
5. On the Network Connection Type page, select **Set up an advanced connection**. Click **Next**.
6. On the Advanced Connection Options page, select **Accept incoming connections**. Click **Next**.
7. On the Devices for Incoming connections page, select the communication device(s) for this connection object. Devices with a marked checkbox will be used by this object; devices with an empty checkbox will not. Click **Next**.
8. On the Incoming VPN Connection page, select whether to allow VPN connections or not. Click **Next**.
9. On the User Permissions page, select users to be allowed to connect over this incoming connection object. Only users marked will be able to use this connection object. Click **Next**.

10. On the Networking Software page, select those components to bind to the incoming connection object. The defaults are usually satisfactory. Click **Next**.
11. Click **Finish**. The new incoming connection object is added to the Network Connections utility awaiting a dial-in attempt.

Project 8-5

To create a direct connect connection object:

This hands-on project requires two systems in close proximity. One system should be labeled as the host or server; the other system should be labeled as the guest or client. A connecting parallel or serial cable or properly oriented infrared link must be present between the two systems.

1. Go to the system that will act as the host in the direct connection pair. Typically, the host system has the resource that needs to be transferred or accessed by the guest system.
2. Open the **Control Panel** (**Start**|**Control Panel**). Click **Switch to Classic View** if the Control Panel is currently in Category View.
3. Double-click **Network Connections**.
4. Launch the New Connection Wizard by double-clicking on the **Create a new connection** link in the Quick List.
5. The first page of the Wizard is a welcome message. Click **Next**.
6. On the Network Connection Type page, select **Set up an advanced connection**. Click **Next.**
7. On the Advanced Connection Options page, select **Connect directly to another computer**. Click **Next.**
8. On the Host or Guest? page, select **Host**. Click **Next**.
9. On the Connection Device page, select the link device type (serial, parallel, infrared, etc.) from the pull-down list. Click **Next**.
10. On the User Permissions page, select the user(s) that can connect over this link. Click **Next**.
11. Click **Finish**.
12. Go to the system that will act as the guest in the direct connection pair.
13. Open the Control Panel (**Start**|**Control Panel**). Click **Switch to Classic View** if the Control Panel is currently in Category View.
14. Double-click **Network Connections**.
15. Launch the New Connection Wizard by double-clicking the **Create a new connection** link in the Quick List.
16. The first page of the Wizard is a welcome message. Click **Next**.

17. On the Network Connection Type page, select **Set up an advanced connection**. Click **Next**.
18. On the Advanced Connection Options page, select **Connect directly to another computer**. Click **Next**.
19. On the Host or Guest? page, select the **Guest** option. Click **Next**.
20. On the Connection Name page, provide a name for this connection object, such as **Lab direct guest 1**. Click **Next.**
21. On the Select a Device page, select the link device type (serial, parallel, infrared, etc.) from the pull-down list. Click **Next**.
22. On the Connection Availability page, select whether this connection will be available for Anyone's use or My use only. Click **Next.**
23. Click **Finish**. The New Connection Wizard completes the connection object creation (i.e., it now appears in the Network Connections window), but instead of returning you to the Network Connection window, the Wizard launches the new connection object for the first time.
24. The Connect dialog box appears. Provide a name and password (for a user account granted access to connect back in step 10). Click **Connect**.

Project 8-6

To Install Internet Information Server on a Windows XP Professional system:

1. Open the **Control Panel** (**Start**|**Control Panel**). Click **Switch to Classic View** if the Control Panel is currently in Category View.
2. Launch the **Add or Remove Programs** applet by double-clicking on its icon.
3. Select the **Add/Remove Windows Components** item in the left column. This launches the Windows Components Wizard.
4. Select the checkbox beside Internet Information Services (IIS). Click **Next**.
5. When prompted, provide the path to the Windows XP Professional CD. This can involve just inserting the CD into the drive and clicking **OK** or using a Browser dialog box to locate the \i386 directory on the CD.
6. The installation Wizard copies files to your system. This can take several minutes. You might be prompted for the path to the CD a second time. Eventually, click **Finish**.
7. Click **Close** to terminate the Add or Remove Programs applet.
8. Close the Control Panel by selecting **File**|**Close**.

Project 8-7

To manage resources hosted by a Web server:

1. Open the **Control Panel** (**Start**|**Control Panel**). Click **Switch to Classic View** if the Control Panel is currently in Category View.
2. Double-click **Administrative Tools**.
3. Double-click **Internet Information Services**.
4. Expand the left node items by double-clicking on them until you can see Default Web Site.
5. Select **Default Web Site**.
6. Select **Action**|**Properties**.
7. Select the **Home Directory** tab.
8. In the box labeled **Local Path,** take note of the directory path listed there. It will most likely be "c:\inetpub\wwwroot." This is the top-level root directory for your Web site.
9. Click **OK**.
10. Select **File**|**Exit** to close the IIS tool.
11. Launch Windows Explorer (**Start**|**All Programs**|**Accessories**|**Windows Explorer**).
12. Locate the top-level root directory for your Web site and select it in the left pane of Windows Explorer.
13. In the right pane of Windows Explorer right-click over an empty area, select **New** from the pop-up menu, then select **Text Document** from the fly-open menu.
14. Type in the filename **default.htm**, then press **Enter**. If prompted about whether to change the filename extension, click **Yes**.
15. Open Notepad (**Start**|**All Programs**|**Accessories**|**Notepad**).
16. Select **File**|**Open**.
17. Change the Files of type pull-down list to **All Files**.
18. Locate and select the **default.htm** document.
19. Click **Open**.
20. Type the following into the body of this document: **<HTML><BODY>This is the default document.<P></BODY></HTML>**.
21. Select **File**|**Save**.
22. Select **File**|**Exit**.
23. Launch Internet Explorer from the desktop by double-clicking its icon.
24. Select **File**|**Open**.
25. Type **localhost** and click **OK**.

26. The Web browser should display the default document you created by showing a line stating "This is the default document."
27. Select **File|Close**.

Project 8-8

To configure Internet Connection Sharing:

This hands-on project requires that a network connection already be defined.

1. Open the **Control Panel** (**Start|Control Panel**). Click **Switch to Classic View** if the Control Panel is currently in Category View.
2. Double-click **Network Connections**.
3. Select the predefined dial-up connection item from the Network Connections tool.
4. Select **File|Properties**.
5. Select the **Advanced** tab.
6. Select the **Allow other network users to connect through this computer's Internet connection** checkbox under Internet Connection Sharing.
7. A message dialog box might appear stating that a username and password are not stored for this connection. Click **OK**.
8. Click the **Settings** button.
9. Select the **Services** tab.
10. Select the checkbox beside **Remote Desktop**.
11. Click **OK**.
12. Click **OK**.

Project 8-9

To configure Internet Connection Firewall:

This hands-on project requires that a network connection already be defined.

1. Open the **Control Panel** (**Start|Control Panel**). Click **Switch to Classic View** if the Control Panel is currently in Category View.
2. Double-click **Network Connections**.
3. Select the predefined dial-up connection item from the Network Connections tool.

4. Select **File**|**Properties**.
5. Select the **Advanced** tab.
6. Select the **Protect my computer and network by limiting or preventing access to this computer from the Internet** checkbox under Internet Connection Firewall.
7. Click **Settings**.
8. On the Services tab, mark any service that you want ICF to pass without restriction.
9. Select the **Security Logging** tab.
10. Mark the **Log dropped packets** checkbox.
11. Select the **ICMP** tab.
12. Make sure that all checkboxes are cleared.
13. Click **OK**.
14. Click **OK** again.

CASE PROJECTS

1. Your organization has decided to allow several employees to work from home. With Windows XP Professional on the telecommuters' systems, describe your configuration and setup options, including how you can deal with security and non-dedicated connections.
2. After installing a new modem, none of your connection objects will function, even after you've recreated them. Describe the process you would use to troubleshoot this problem.